U.S. House of Representatives

Committee on Transportation and Infrastructure

Subcommittee on Aviation

Using Biometrics to Improve Aviation Security

Testimony by

Richard E. Norton
Executive Vice President

May 19, 2004

National Biometric Security Project
Suite 390 South
601 13th Street, N.W.
Washington, DC 20004
(202) 347-9788

About NBSP and Biometric Research

The National Biometric Security Project (NBSP) is a nonprofit research foundation that was established in 2002 to improve national security by developing and deploying advanced biometric technologies. The specific mission of the NBSP is to provide the Federal Government with research and development capabilities that will give the civilian government and private sector critical infrastructure the tools needed to secure facilities and sensitive data from compromise and intrusion by unauthorized people.

NBSP, headquartered in Washington, DC, is primarily funded under an appropriation by Congress under the Biometrics in National Security program. NBSP maintains a major testing and research center in Morgantown, West Virginia. Our primary activities are focused in five major areas:

1. Conducting applied research to determine security requirements, and developing solutions that can be implemented under rigorous operational conditions.
2. Establishing training and education programs to develop U.S. expertise in biometric technology.
3. Testing and evaluating biometric products to determine if they can fulfill operational requirements.
4. Maintaining and distributing information about biometric products and how they can be used to meet security needs.
5. Establishing standards that will simplify the tasks of selecting, implementing and operating biometric-based security solutions in real-world environments.

Biometrics and Aviation Security: Lessons Learned

Biometrics have been in use at airport facilities for over a decade. Federal aviation regulations have long supported the installation of biometric systems to guard sensitive areas of airports against intrusion, and a significant body of information exists on how airports have managed the processes of deploying, operating and administering biometric-based security solutions.

The most prominent example is offered by San Francisco International Airport, which uses over 170 biometric devices to protect ramps and jetways against unauthorized access. Employees who are enrolled in the system use a combination of a personal information number or ID card and their biometric (in this case, hand geometry) to gain admittance to secure areas. According to airport officials the system operates reliably under demanding conditions. Major airports in New York, Los Angeles, Chicago, Miami and Newark have also used biometrics to varying degrees to upgrade security.

As noted above, Federal regulations clearly supported the use of biometrics to enhance security levels at airports since the early 1990s. However, since the regulations only offered biometrics as one of several options for complying with security requirements, they have not been deployed as part of a mandatory program. Following the events of September 11, however, Congress took decisive steps to accelerate the installation of biometric-based security solutions and mandated trials of biometrics to secure the airport footprint. Under the Airport Access Control Pilot Program, the Transportation Security

Administration (TSA) will evaluate how biometric devices operate when they are installed at 20 airports throughout the U.S. beginning later this year. Metrics from that program should provide key indicators on the effectiveness of a wide array of biometrics. Among the most critical of these will be "usability" measurements that compare ease of operation against the business and security imperatives of the aviation industry.

Large-Scale Deployment: The Next Challenge

Putting biometrics into service at a particular airport is a question that has already been largely answered. Based on the years of experience acquired at San Francisco, NBSP expects that the existing body of data combined with the results of the TSA trials should clearly settle any lingering doubts about whether biometrics can significantly improve security controls at any given commercial airport. In situations where these systems are used daily by a trained group of users, biometrics have proven to be a particularly effective means of discouraging attempts to gain unauthorized access to facilities.

The challenge will be to settle on a model that will allow biometrics to be used effectively on a national basis by a broad group of transportation workers. Requiring those with regular access to a specific airport to enroll in a biometric security system presents no significant cost, administrative or procedural barriers. Expanding coverage to a national infrastructure level raises several major issues to be resolved:

- How to make biometric systems interoperable without mandating that a particular biometric solution be used across the board;
- How to ensure that people are not enrolling under an assumed identity or with multiple identities;
- How to implement a national system on a cost-effective basis; and
- How to guarantee that privacy requirements can be met and that data is adequately safeguarded against compromise and abuse.

The TSA has started to work on these issues under the auspices of the Transportation Worker Identity Card (TWIC) program. The TWIC concept calls for the issuance of a card to all transportation employees, including those who must have access to airport facilities in the performance of their duties. To date, TSA has established a concept of operations for the TWIC program, which calls for applicants to be pre-screened for multiple identities and criminal record through the use of fingerprint and face recognition biometrics. This is an essential process that can be met through the use of existing biometric technology.

Beyond the enrollment stage, the TWIC architecture will accommodate the use of other biometrics to perform the key task of controlling access in an operational environment. The design will permit an airport to incorporate its existing biometric door access systems within the TWIC design, or make use of different biometrics to solve specific operational requirements as they are identified. This ability to upgrade or change technologies seamlessly as new capabilities are developed is a necessary attribute of any well-designed security system.

Following its research on card types operational concepts, TSA is actively examining the existing infrastructure that is in place at transportation facilities nationwide, with a view to leveraging capabilities and resources that are already in place. NBSP agrees that this is a wise approach. Creating a standalone TWIC program from scratch would be prohibitively expensive, and local expertise will provide important insight on how the system can be installed without disrupting economically vital transportation systems.

Pre-Deployment Biometric Testing and Research Support

As these critical tasks move forward and biometric-based solutions come closer to full-scale implementation at airports, NBSP is actively leading a number of initiatives that should help ease problems with deployment. As a first step, NBSP is accelerating the development of standards that will enable biometric data to be accurately stored and accessed in a wide variety of systems. Working with the National Institute of Standards and Technology (NIST) and international standards organizations, NBSP has placed a top priority on assuring that interoperability problems are removed as a barrier to the broad adaptation of biometric technology.

Next, NBSP is equipped to handle the demands of a testing regime that can evaluate and certify the effectiveness of biometric products and solutions prior to field installation. NBSP laboratories are being designed to subject devices and integrated systems to stringent examinations that will determine if they can operate under a wide range of conditions. These tests will include evaluations of usability, durability, sensitivity to ambient environmental conditions, and performance against established requirements.

Finally, NBSP is building a cadre of trained biometrics professionals who can assist government and the private sector critical infrastructure to develop requirements for biometric systems and oversee their installation. Together with NBSP's database of information on biometric technologies and applications, the Project offers Federal, state, and local authorities an unprecedented capability that can help them speed up the adoption of practical, effective solutions that use biometrics to achieve new levels of security.

We appreciate this opportunity to testify before the Subcommittee on Aviation concerning this vital topic, and look forward to answering any questions you may have.